InCharge™

ATM/Frame Relay Availability Manager User Guide

Cisco Part Number: OL-6058-01

Contents

Preface

This guide provides detailed information about InCharge ATM/Frame Relay Availability Manager (InCharge ATM/Frame Relay AM or IC ATM/FR AM). InCharge ATM/Frame Relay AM automatically diagnoses connectivity failures in managed networks. A connectivity failure occurs when one element in the network is unable to communicate with another.

Refer to "Connectivity Failures Diagnosed" on page 15 for a list of specific problems diagnosed by InCharge ATM/Frame Relay Availability Manager.

Intended Audience

This guide is intended to be read by IT managers seeking to better understand the value of InCharge ATM/Frame Relay AM, by system administrators configuring and using the application, and by operators receiving and acting upon notifications.

Prerequisites

It is assumed that InCharge ATM/Frame Relay AM and one or more InCharge consoles are installed. For information on installing InCharge ATM/Frame Relay AM or InCharge consoles, refer to your installation guide.

Document Organization

This guide consists of the following.

1. Introduction	Presents the concepts and challenges of managing network connectivity and describes InCharge ATM/Frame Relay AM.
2. Managed Elements and Their Relationships	Describes the network elements managed by InCharge ATM/Frame Relay AM.
3. Connectivity Failures Diagnosed	Describes the failures diagnosed by InCharge ATM/Frame Relay AM.
4. Default Settings	Provides information about the default settings used to configure InCharge ATM/Frame Relay AM.
A. Symptomatic Events	Describes the symptomatic events diagnosed by InCharge ATM/Frame Relay AM.
B. Diagnosis of Unstable Elements	Describes how InCharge concludes that a system or network adapter is unstable.
C. Alarms Processed	Identifies the alarms that InCharge ATM/Frame Relay AM collects and processes.

Table 1: Document Organization

Documentation Conventions

Several conventions may be used in this document as shown in Table ?.

CONVENTION	EXPLANATION
`sample code`	Indicates code fragments and examples in Courier font
keyword	Indicates commands, keywords, literals, and operators in bold
`%`	Indicates C shell prompt
#	Indicates C shell superuser prompt
<parameter>	Indicates a user-supplied value or a list of non-terminal items in angle brackets
[option]	Indicates optional terms in brackets
/InCharge	Indicates directory path names in italics
yourDomain	Indicates a user-specific or user-supplied value in bold, italics
File > Open	Indicates a menu path in italics

Table 2: Documentation Conventions

In this document, the term ***BASEDIR*** represents the location where InCharge software is installed. The term ***BASEDIR*** represents the */opt* directory for UNIX, the *C:\InCharge* directory for Windows, or your specified path. The InCharge software resides in the ***BASEDIR****/smarts* subdirectory.

Directory path names are shown with forward slashes (/). Users of the Windows operating systems should substitute back slashes (\) for forward slashes.

Also, if there are figures illustrating consoles in this document, they represent the consoles as they appear in Windows. Under UNIX, the consoles appear with slight differences. For example, in views that display items in a tree hierarchy such as the Topology Browser, a plus sign displays for Windows and an open circle displays for UNIX.

1

Introduction

InCharge ATM/Frame Relay Availability Manager (InCharge ATM/Frame Relay AM) collects and correlates alarms that are generated as a result of a failure in a wide area network, pinpoints the failed element, and identifies all of the elements affected by the failure. With InCharge ATM/Frame Relay AM, you can focus on a failed element, prioritize it by its impact, and address its resolution in a time- and cost-efficient manner.

Wide Area Networks (WANs)

InCharge ATM/Frame Relay AM monitors WANs. WANs are complex, highly redundant networks that cover large geographical areas. Commonly, they utilize both physical and logical elements to transfer multiple types of data from one point to another.

Figure 1 illustrates the topology of a typical WAN. The WAN is enclosed within a cloud. The network provides connectivity between routers which, in turn, function as access points to other devices. In the figure, Router 1 provides connectivity between the WAN and the IP Network on which the management station is located.

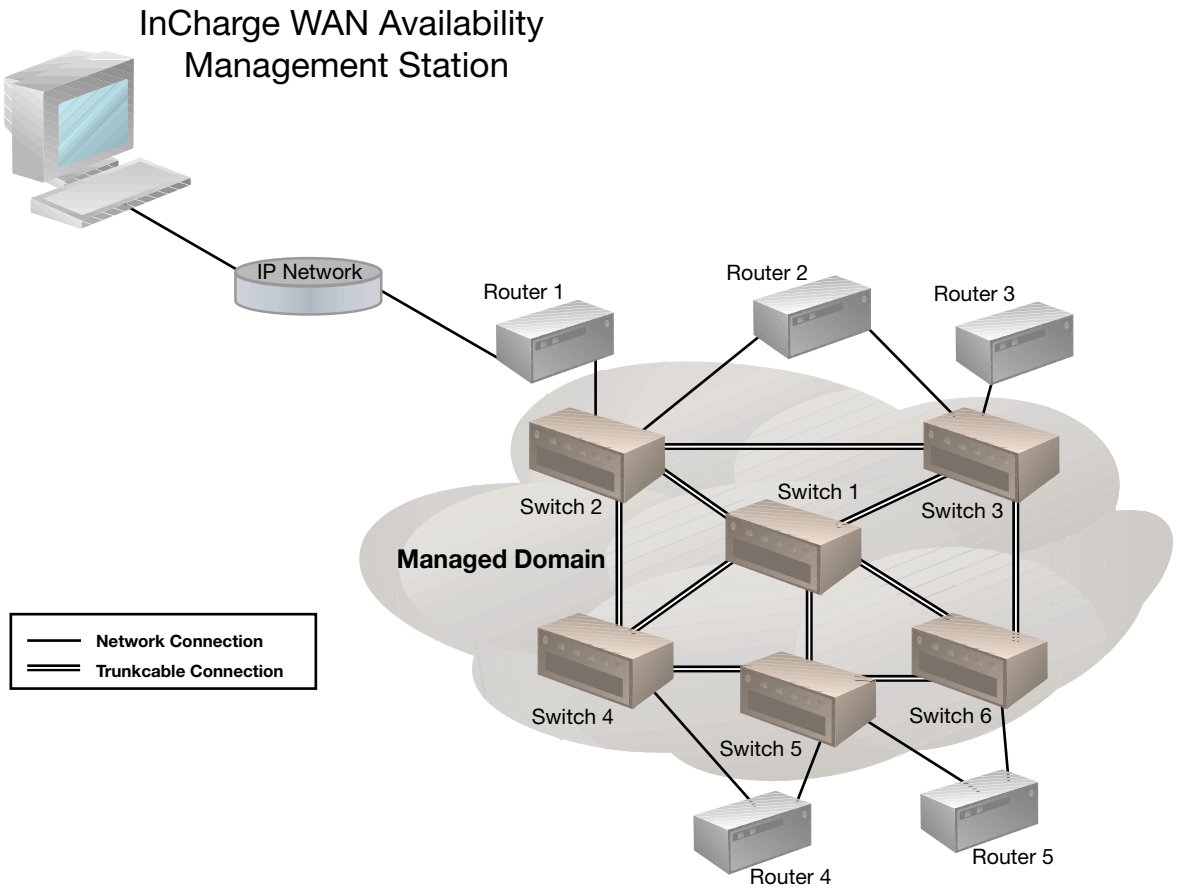

Figure 1: Typical WAN Architecture

Physical Elements

The physical elements of a WAN are the real-world devices that plug together and provide the physical connectivity between points in the network. The physical elements include: switches, cards, physical ports, and trunk cables.

Figure 2 depicts the physical connectivity of a sample WAN.

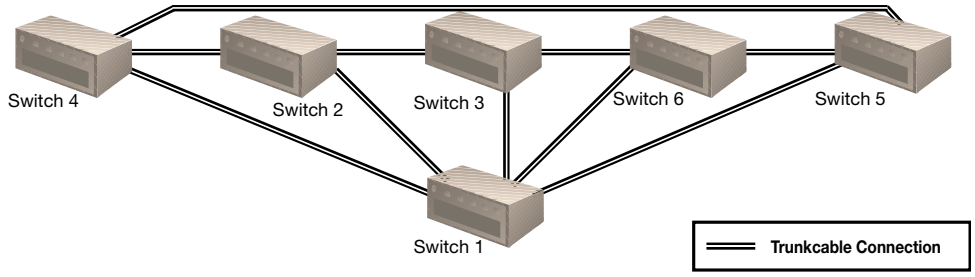

Figure 2: WAN Physical Connectivity

Logical Elements

The logical elements of a WAN are service access points and non-physical connections that are software configured and layered over the physical elements. The logical elements include: logical ports (layered over physical ports), permanent virtual circuits, or PVCs (that connect logical ports), and logical trunks (pre-configured sets of trunk cables that establish a physical path between a pair of logical ports).

Figure 3 depicts four PVCs defined in the WAN shown in Figure 2. It is important to note that PVCs are not permanently bound to a particular physical path; the actual path that the data flows across can change dynamically depending on the failures and/or load in the network.

For example, the data that flows across PVC S4S6 in Figure 3 can take any of the following paths:

- S4, S2, S3, S6
- S4, S1, S6
- S4, S2, S1, S6
- S4, S2, S3, S1, S6
- S4, S5, S6

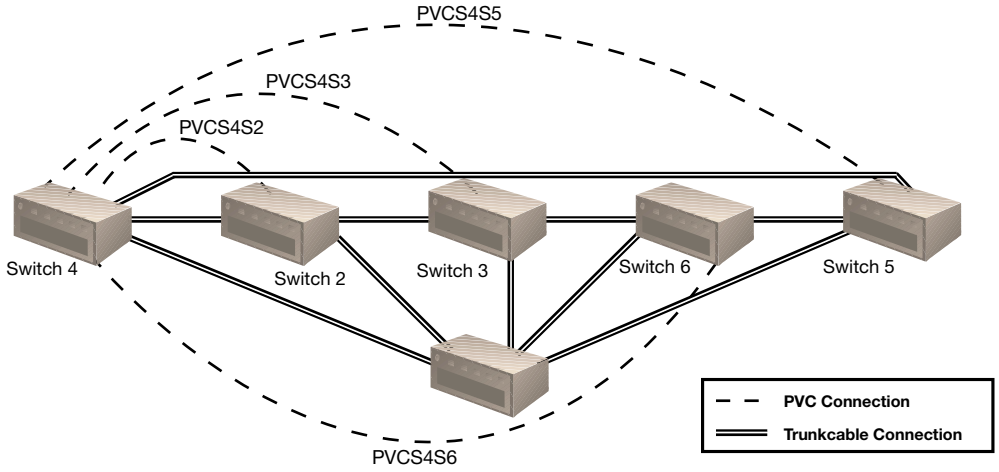

Figure 3: Permanent Virtual Circuit (PVC) Connectivity

Figure 4 depicts three logical trunks defined in the WAN shown in Figure 2. Unlike PVCs, logical trunks are bound to a given physical path, and the configuration of the path cannot change dynamically. Should a failure occur that breaks the connectivity of a path established for a logical trunk, the logical trunk fails, and must be manually re-configured before information can flow again.

In Figure 4, for example, the data that flows across the logical trunk LTS4S3 uses the physical trunks between Switch 4 and Switch 2, and between Switch 2 and Switch 3. Should any of these physical connections fail, the data cannot flow across the logical trunk LTS4S3, even though there is physical connectivity between Switch 4 and Switch 3 using alternative paths.

Similarly, the logical trunk LTS3S5 is configured to use the physical trunks between Switch 3 and Switch 6, and between Switch 6 and 5.

The logical trunk LTS4S6 uses the physical trunks between Switch 4 and Switch 1, and between Switch 1 and Switch 6.

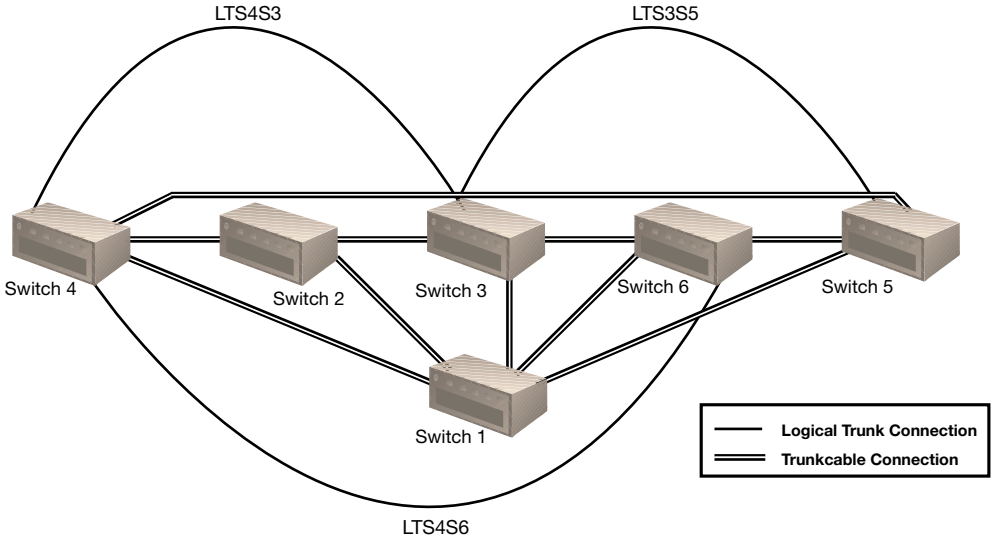

Figure 4: Logical Trunk Connectivity

Figure 5 depicts all of the physical and logical connectivity defined for the WAN in Figure 2. It shows the PVCs as well as the logical trunks established for the network. It is important to note that some PVCs may use the defined logical trunks, while others do not, depending on how they are configured.

For example, PVCS4S5 may use the logical trunks LTS4S3 and LTS3S5, while the PVCS4S6 does not utilize the logical trunk LTS4S6.

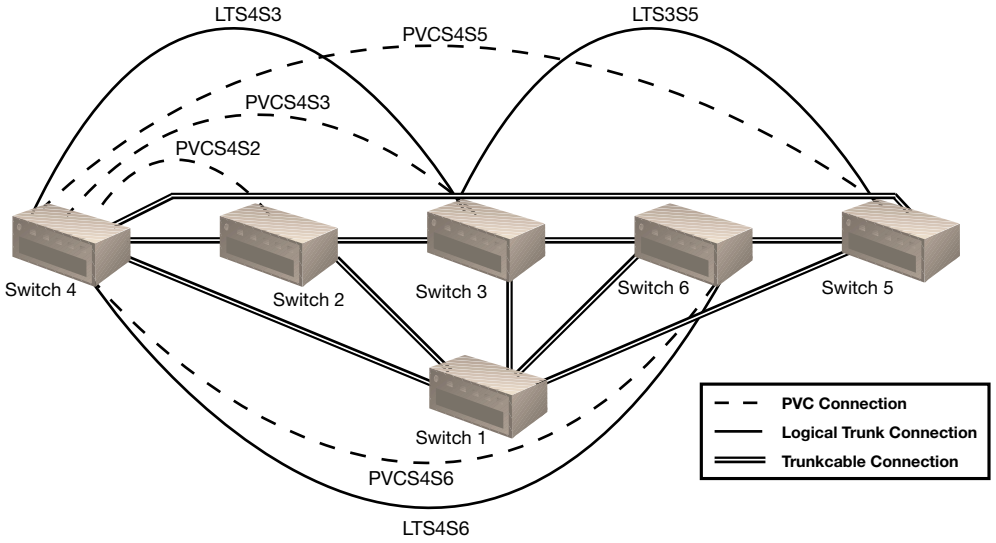

Figure 5: Physical and Logical Connectivity

InCharge ATM/Frame Relay AM

InCharge ATM/Frame Relay AM diagnoses connectivity failures in switched WANs. The networks typically utilize either Frame Relay (FR) or Asynchronous Transfer Mode (ATM) technology. Both are capable of carrying multiple types of data across great distances at very high speeds.

InCharge ATM/Frame Relay AM manages both the physical and logical elements of the networks. That means that it observes and monitors the network elements that are configured by software, as well as the actual switches, cards, and ports that carry data.

The network elements managed by InCharge ATM/Frame Relay AM include:

- Switches
- Cards
- Logical Ports
- Logical Trunks
- Permanent Virtual Circuits (PVCs)

- Physical Ports
- Trunk Cables

InCharge Monitoring

InCharge ATM/Frame Relay AM monitors the network by listening for notifications sent by the devices. The InCharge application then uses the notifications to diagnose the failed elements that are breaking network connectivity.

InCharge Notifications

InCharge ATM/Frame Relay AM reports three types of notifications: root-cause failures, symptomatic events, and compound events. Root-cause failures indicate diagnosed problems. Symptomatic events indicate abnormal conditions and are used by InCharge ATM/Frame Relay AM to diagnose root-cause failures. Compound events summarize when one or more events are associated with a high-level network element or any of the element's lower level constituents. For example, a compound event notification is generated for a switch when a card in the switch has a problem or the switch itself is down.

Notifications are displayed in the alarm log view of the InCharge Monitoring Console. Root-cause failures are colored red in the alarm log. Symptomatic events are colored orange in the alarm log. Compound events are colored purple in the alarm log.

WAN Failure Example

For example, consider the failure of Switch 6 in the network shown in Figure 6. A failure in Switch 6 causes the following to occur:

- It breaks the physical connections to all immediately connected devices (Switches 1, 3, and 5)
- It breaks all logical connections that either originate or terminate on Switch 6 (PVCS4S6, and the logical trunk LTS4S6)
- It breaks the connection of logical trunk LTS3S5 that was configured to use the physical trunks between Switches 3 and 6, and between Switches 6 and 5

The management station does not receive any notifications directly from Switch 6, and does not receive any response from the device that it tries to reach. However, the management station receives notifications from the immediately connected devices that indicate the loss of physical connectivity (to Switches 1, 3, and 5) from the logically connected devices (Switches 3, 4, and 5) which have lost logical connectivity as a result of the failure.

InCharge ATM/Frame Relay AM uses its comprehensive understanding of the WAN's physical and logical connectivity in order to:

- Correlate all symptomatic notifications
- Pinpoint the root-cause problem: Switch 6 Down
- Calculate the impact of the failure on the WAN's physical and logical trunks, and PVCs

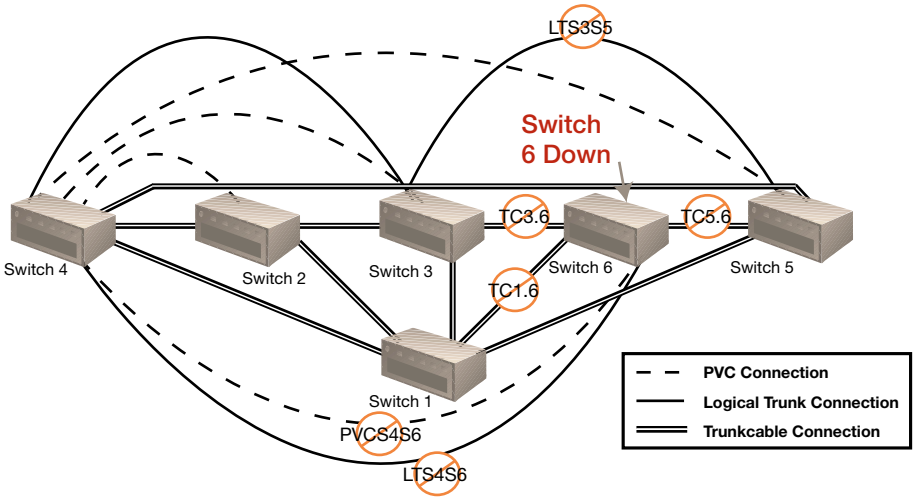

Figure 6: Example of a WAN Switch Failure

LAN/WAN Management Differences

The management of local area networks (LANs) and WANs is fundamentally different.

- In a LAN environment, a network management station monitors the network by periodically polling every network element, and checking

the status of each element's components (for example, interface, port, or card).

In a WAN environment, the sheer density of ports per device, along with the few CPU cycles that can be dedicated to answering management requests, make continuous polling impractical. The network management station must rely on the notifications sent by devices to diagnose root-cause problems.

- Typically, a LAN environment is not completely redundant: it does not support a fully meshed topology with redundant paths. Therefore, the failure of a single element may cause hundreds of devices to become unreachable. The failed element breaks the connectivity between the management station and all of the devices accessed through the failed device. During the polling cycle, the management station generates a notification for every unreachable element.

  Because of the inherent redundancy in a WAN environment, the failure of an element causes minimal impact. In most cases, only the uniquely connected devices are unreachable; the network automatically finds alternate paths to reach healthy devices. Consequently, the number of notifications generated by a failure are greatly reduced. Root-cause diagnostic analysis must be accomplished based on a limited number of symptoms, a much smaller number than the symptoms in a LAN.

2

Managed Elements and Their Relationships

This chapter describes the network elements discovered and managed by InCharge ATM/Frame Relay AM, along with the relationships between the elements. Elements are categorized into the following groups: connections, containers, systems, network adapters, service access points, and logical links.

Note: The following network element descriptions are based on concepts and element classifications as defined by the InCharge Common Information Model (ICIM). ICIM is an implementation of the Common Information Model (CIM) developed by the Distributed Management Task Force, Inc. (DMTF).

Connections

A connection is any link between network adapters. (For more information, see "Network Adapters" on page 12.) The following connection is managed by InCharge ATM/Frame Relay AM:

- *Trunk Cable* – A trunk cable, or physical trunk, is a connection between two physical ports. Trunk cables provide the physical connectivity for logical links. (For more information, see "Logical Links" on page 13.) Switches are often trunked to connect multiple segments or to provide redundant pathways through the network.

Containers

A container is a physical package that contains or hosts other components.

- *Card* — A card is a physical module or blade of a networking device.

Systems

A system is a logically complete group of elements that provide services to users or other systems.

- *Switch* — A switch is a network element that switches packets, typically at wire speeds, between physically separate network segments.

Network Adapters

A network adapter is a logical or physical component of a network device at which the device connects to a network. Physical ports are examples of network adapters.

- *Physical Port* – A port is a specific place at which a connection to a network segment can be made. A network adapter connects to a port to gain access to its network segment. For example, a physical trunk is connected to an ATM Switch at one of the switch's physical ports.

Service Access Points

A service access point is a communication endpoint of a network element (for example, logical ports on a physical port from which data can be sent and received). Service access points represent the abstraction of a switch's physical port so that it can be related to a logical link.

- *Logical Port* – A logical port represents a listening or sending endpoint used by network services to transmit data over a logical link.
- *IP* – An IP endpoint describes the IP layer characteristics of a network-attached interface. An IP endpoint is designated by a unique IP address.

Logical Links

A logical link represents a connection between network nodes. The communication between nodes is governed by the protocol rules of the network layer in which the link exists (for example, an ATM trunk in the link layer).

- *Permanent Virtual Circuit* – A PVC represents a permanent virtual circuit established between two logical ports. The data traverses one or more physical trunks from one logical port or end point to another in the PVC. The particular physical trunks that the data traverses depends on the current state of the network. Most WAN devices automatically reconfigure the physical path of a PVC when failures occur.
- *Logical Trunk* – A logical trunk represents the connectivity between a pair of logical ports. It is very similar to a PVC. Unlike a PVC, however, the physical path used by a data communication over a logical trunk is defined during the configuration of the trunk, and does not automatically change when failures occur.

Relationships

The following relationships exist between the managed elements.

- *ConnectedVia/ConnectedTo (Logical Port/Logical Link)* – The relation between a Logical Port and the Logical Link to which it connects (for example, a PVC or a Logical Trunk). The cardinality of the relation is

one to many. A Logical Link may be connected to more than one Logical Port.

- *PackagesSystems/SystemPackagedIn (Chassis/Systems)* – The relation explicitly defines the association between systems and the physical packages that realize them. The cardinality of the relation is many-to-many.
- *Peer/Peer (PhysicalPort/PhysicalPort)* – The Peer relationship between physical ports indicates that two physical ports are connected to each other. It is computed using the stored relationshipset ConnectedVia.
- *Peer/Peer (LogicalPort/LogicalPort)* – The Peer relationship between logical ports indicates that two logical ports are connected to each other. It is computed using the stored relationshipset ConnectedVia.
- *LayeredOver/Underlying (Logical Trunk/Physical Trunk)* – The LayeredOver/Underlying relation describes the notion that Elements in a higher layer use the services of, or are implemented by, Elements in lower layers.

  For example, the relation between Elements representing a protocol stack. Elements in a higher layer are functionally dependent on the health of underlying Elements. The cardinality of the relation is many to many.
- *ComposedOf/PartOf (Switch/Card)* – ComposedOf is the relation that defines the elements contained within another element.
- *ComposedOf/PartOf (Card/Physical Port)* – ComposedOf is the relation that defines the elements contained within another element.
- *Realizes/RealizedBy (Card/Physical Port)* – Realizes/RealizedBy is the relation that defines the mapping between a Logical Device and the physical components that implement the Device.
- *LayeredOver/Underlying (Logical Port/Physical Port)* – LayeredOver/Underlying is the relation that describes the notion that Elements in a higher layer use the services of, or are implemented by, Elements in lower layers.

  For example, the relation between Elements representing a protocol stack. Elements in a higher layer are functionally dependent on the health of underlying Elements. The cardinality of the relation is many to many.

3

Connectivity Failures Diagnosed

InCharge ATM/Frame Relay AM diagnoses connectivity failures in managed elements and makes it possible to quickly identify root-cause failures in a managed network. Root-cause failures indicate problems that require immediate attention. InCharge correlates the apparent failures of other elements reached through the failed element to the root cause and only notifies you of the origin of the problem.

This chapter describes the problems (root-cause failures) and compound events diagnosed for each element managed by InCharge ATM/Frame Relay AM.

Table 3 summarizes the notifications generated for each managed element. Refer to "Managed Elements and Their Relationships" on page 11 for a complete description of all elements managed by InCharge ATM/Frame Relay AM.

Network Element	Notification	
	Failure	Compound
Connections		
Trunk Cable	Down Unstable	
Containers		
Card	Down	
Systems		
Switch	Down Unstable	Connectivity Exception
Network Adapters		
Physical Port	Down Unstable	
Service Access Points		
Logical Port	Down	
Links		
Logical Trunk	Down	
PVC	Down	

Table 3: Connectivity Diagnosis Summary

Connections

A connection can be a trunk cable. Problems diagnosed for a connection include Down and Unstable.

Connection Down

Down indicates that one or both network adapters linked by the connection have failed or the trunk itself is broken. A connection failure breaks connectivity between the management station and each network adapter it links, generating symptomatic events at both ends.

A *Trunk Cable Down* notification supersedes a *Physical Port Down* notification if a trunk cable connects a port that is down.

Trunk Cable Down Scenario

Figure 7 depicts a network site where six switches are connected. The figure shows what happens when the trunk cable connecting Switch 1 and Switch 3 goes down.

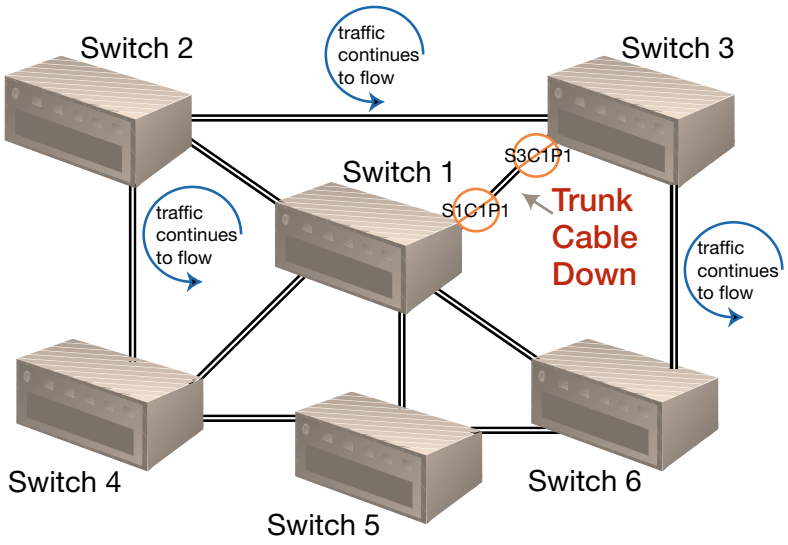

Figure 7: Trunk Cable Down

Since Switch 2 and Switch 6 provide alternate paths for the network traffic to flow from and to Switches 1 and 3, connectivity is not lost between any devices. The management station can successfully reach each device.

InCharge ATM/Frame Relay AM intelligently analyzes port status and can correlate port failures to other root-cause problems. In this instance, InCharge ATM/Frame Relay AM identifies two symptoms—apparent port failures on Switch 1 and Switch 3. This example illustrates the power of Data Link (Layer 2) correlation to diagnose a problem that may have otherwise gone unnoticed: the Trunk Cable Connection between a port on Switch 1 (S1C1P1) and a port on Switch 3 (S3C1P1) is down.

Connection Unstable

Unstable indicates that one or both network adapters linked by the connection are unstable. A network adapter is considered unstable if it alternates between up and down states over a short period of time.

A *Trunk Cable Unstable* notification supersedes a physical *Port Unstable* notification if a trunk cable connects a port that is unstable.

Network Connection Unstable Scenario

Figure 8 depicts a sample network where only three devices are shown. At one end, Switch 1 provides dual frame relay connections to Switch 2 and Switch 3. This figure illustrates what happens when a trunk cable becomes unstable. Switches 1 and 2 will generate notifications that ports S1C1P1 and S2C1P1, respectively, have changed status, either going down or coming back up again.

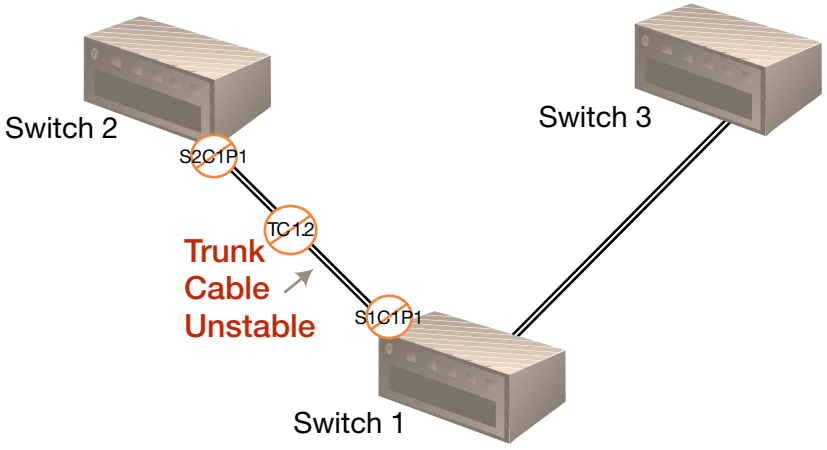

Figure 8: Trunk Cable Unstable

The current scenario is precipitated by a transient switching problem occurring within Switch 1. Switch 1 and Switch 2 keep losing their connection and continually attempt (but fail) to reestablish it. InCharge ATM/Frame Relay AM observes the instability of this connection by continually receiving notifications from Switch 1 and Switch 2 that indicate the change of status on the ports connected to the trunk cable.

InCharge ATM/Frame Relay AM correlates the repeated notifications sent by the switches and consolidates it into one problem notification: a trunk cable between a port on Switch 1 (S1C1P1) and a port on Switch 2 (S2C1P1) is unstable.

Systems

An example of a system is a switch.

Problems diagnosed for a system failure include Down and Unstable. A Connectivity Exception compound event is also diagnosed for a system.

System Down

Down indicates that a system has failed. A system failure causes all ports on the system and all elements accessed through the system to be unreachable.

Switch Down Scenario

Figure 9 depicts a network site in which several switches are connected. Switch 1 connects to all switches in the shown network. The figure shows what happens when Switch 1 fails.

A redundant path exists from InCharge ATM/Frame Relay AM to Switches 2, 3, and 4. However, Switches 5 and 6 can only be reached through Switch 1.

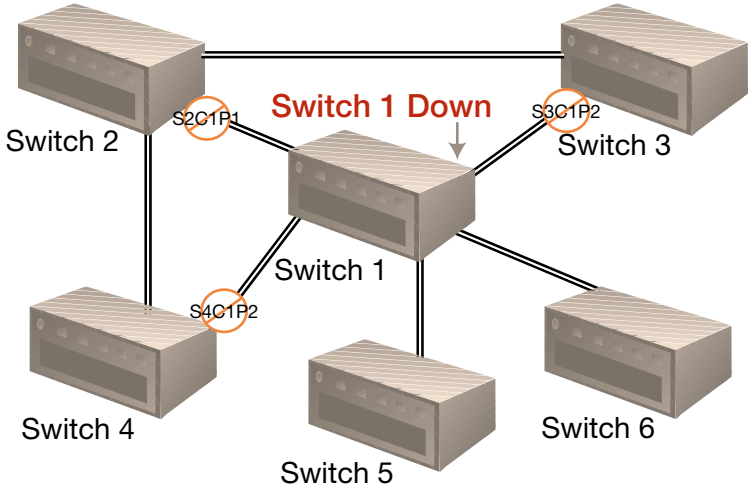

Figure 9: Switch Down Scenario

Many alarms are generated when Switch 1 fails, making an accurate analysis a challenge.

InCharge ATM/Frame Relay AM gathers evidence from the surrounding devices, observing the following symptomatic events:

- One apparent port failure on Switch 2 (S2C1P1)
- One apparent port failure on Switch 3 (S3C1P2)
- One apparent port failure on Switch 4 (S4C1P2)
- Switches 1, 5, and 6 cannot be reached from the management station

InCharge is able to analyze symptoms involving network traffic flowing *upstream* of the failure (apparent port failures on Switches 2, 3, and 4) as well *downstream* of the failure (the two unresponsive Switches 5 and 6).

A similar, but not identical, set of symptoms defines the card down scenario. (For details see the "Card Down Scenario" on page 21.) In both scenarios the network elements connected to the downed element appear to have failed. Also, all elements downstream of the failed element are unresponsive. InCharge ATM/Frame Relay AM draws a different conclusion this time, however, because the switch itself is unresponsive.

System Unstable

Unstable indicates that a system has repeatedly restarted over a short period of time and is considered unstable. The Restart Trap Threshold and the Restart Trap Window parameters in the Connectivity setting control the analysis for a system unstable condition.

For more information about these parameters, refer to "Connectivity" on page 27.

For more information about how InCharge concludes that a system is unstable, refer to Appendix B, "Diagnosis of Unstable Elements" on page 31.

System Connectivity Exception

Connectivity Exception is a compound event that indicates that one or more connectivity-related root-cause failures exist for a particular system or one of its components. For example, if the system is down or one of its ports is down, a Connectivity Exception will be reported for it.

Containers

A container can be a card. *Down* is the only problem diagnosed for a container failure.

Card

Down indicates that a card has failed. A card failure causes all ports in the card to fail. Failures can include:

- Physical ports in the card
- Physical trunks connected to the ports
- Logical connections that rely upon the physical connectivity provided by the ports in the card

Card Down Scenario

Figure 10 depicts a portion of a network where Switch 1 is physically connected to Switches 2 and 3, and 4. The figure illustrates what happens when a card fails on Switch 1.

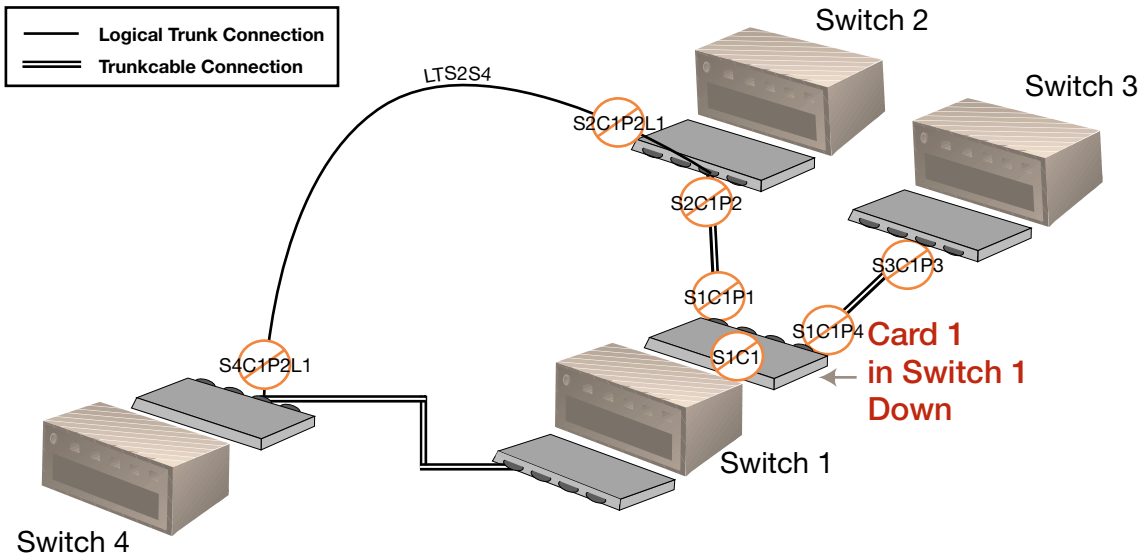

Figure 10: Card Down Scenario

Card 1 contains four ports. Two ports connect, via trunk cables, to Switch 2 and Switch 3. The remaining two ports on the card are unused. On Switch 2, the port connected to Switch 1 is also where a logical trunk to Switch 4 starts.

There are redundant paths between the two switches that are not shown in the diagram. Since data can still pass across the network using an alternate path, the failure of the card in the redundant switch may go unnoticed. Although this card failure does not eliminate network redundancy, it reduces it, putting important devices at risk.

InCharge ATM/Frame Relay AM diagnoses the root cause of the problem by correlating the symptomatic events that can be notified by Switches 1 through 4:

- Four apparent port failures on Switch 1 (InCharge ATM/Frame Relay AM recognizes that S1C1P2 and S1C1P3 are simply unused, but reports S1P1 and S1P4 as operationally down)
- One apparent physical port failure on Switch 2 (S2C1P2)
- One apparent physical port failure on Switch 3 (S3C1P3)
- A notification, generated by Switch 1, indicates that the card module (S1C1) is down
- One apparent logical port failure on Switch 2 (S2C1P1)
- One apparent logical port failure on Switch 4 (S4C1P3)

Instead of analyzing each symptom individually, InCharge views and analyzes these events in their totality. From this totality, the problem's unique signature emerges: Card 1 on Switch 1 is down.

Network Adapters

A network adapter can be a physical port.

Problems diagnosed for a network adapter failure include *Down* and *Unstable*.

Network Adapter Down

Down indicates that a port has failed. A *Port Down* notification is superseded by a *Trunk Cable Down* notification if the port is connected via a trunk cable.

Network Adapter Unstable

Unstable indicates that a port repeatedly alternates between up and down states over a short period of time and is considered unstable. Parameters contained in the Port Flapping setting control analysis for the network adapter unstable condition.

For more information about these parameters, refer to "Port Flapping (Unstable)" on page 27.

For more information about how InCharge concludes that a network adapter is unstable, refer to Appendix B, "Diagnosis of Unstable Elements" on page 31.

A *Port Unstable* notification is superseded by a *Trunk Cable Unstable* notification if the port is connected via a trunk cable.

Service Access Points

A service access point can be a logical port.

Down is the only problem diagnosed for a service access point failure.

Service Access Point Down

Down indicates that a service access point is not responding to status polls sent by the management station and there is no physical failure in the system or any other related network component to explain it.

A logical *Port Down* notification is superseded by a logical *Trunk Down* notification if the logical port is connected via a logical trunk.

Logical Links

A logical link can be a logical trunk or a permanent virtual circuit (PVC). InCharge ATM/Frame Relay AM reports unique problems for each type of logical link network element.

Logical Trunk

Down indicates that one or both logical ports linked by the connection have failed.

A logical *Trunk Down* notification supersedes a logical *Port Down* notification if the logical port is connected through a logical link.

Permanent Virtual Circuit (PVC)

Down indicates that the PVC has lost connectivity, and needs to be re-established.

4

Default Settings

The InCharge configuration process uses settings to assign polling and threshold parameters to the managed elements in your network. These polling and threshold parameters define InCharge management policies.

A *setting* is a collection of parameters common to a particular type of analysis (for example, connectivity polling). A component called a *group* contains zero or more settings and is related to managed elements in your network based on matching criteria. There are two distinct types of groups: Polling Groups and Threshold Groups.

Each member of a group is configured according to the parameters defined in the group's settings. In this way, different polling and threshold values can be applied to different groups of devices.

Default groups and settings are provided with InCharge ATM/Frame Relay AM. This chapter describes the default settings applicable to connectivity. If you are also using an InCharge availability and/or performance application, additional settings will be available.

Polling

The following settings are accessible via the Polling tab of the Polling and Thresholds Console:

- Connectivity Polling (by default, contained in all Polling Groups)

Connectivity Polling

The Connectivity Polling setting configures connectivity monitoring of a system (for example, a hub, bridge, switch, or router). System connectivity is monitored using a combination of ICMP (Ping) requests for IP status and SNMP requests for interface, port, and card status.

The following parameters are included in the Connectivity Polling setting:

Analysis Mode

Analysis Mode enables or disables the connectivity polling. The default is ENABLED.

Polling Interval

The Polling Interval is the time between successive connectivity polls. The default is 240 seconds.

Retries

Retries determines the number of retry connectivity polls to perform when the initial poll fails. The default is 3.

Timeout

Timeout sets the amount of time allowed for the first poll request before it times out. The default is 700 milliseconds. Successive retries use longer times.

Thresholds

The following settings are accessible via the Thresholds tab of the Polling and Thresholds Console:

- Backup Interface Support (by default, contained in the Interface Group - Backup)
- Connectivity (by default, contained in all System Resource Groups)
- Port Flapping (by default, contained in Interface Groups for ATM, Serial, and Other Interfaces)

Connectivity

The Connectivity setting configures connectivity threshold parameters for network adapters (ports and interfaces). It also controls the analysis of systems that repeatedly restart, and are thus considered unstable. For more information about how InCharge concludes that a system is unstable, refer to Appendix B, "Diagnosis of Unstable Elements" on page 31.

Restart Trap Threshold

The Restart Trap threshold sets the number of SNMP cold or warm start traps that must be received within the amount of time set by the Restart Trap Window parameter in order for InCharge to consider a system unstable. The default is 3. A value of 0 turns off restart analysis.

Restart Trap Window

The Restart Trap Window parameter sets the window of time used to monitor a system's repeated restarts. If the number of start traps meets or exceeds the Restart Trap Threshold during this window of time, the system is considered to be unstable. The default is 15 minutes.

Port Flapping (Unstable)

The Port Flapping setting controls the analysis of network adapters (ports and interfaces) that are continually going up and down. Flapping analysis monitors SNMP link down traps to identify a flapping network adapter and then generates a notification to report that it is unstable. For more information about how InCharge concludes that a network adapter is unstable, refer to Appendix B, "Diagnosis of Unstable Elements" on page 31.

The following parameters are included in the Port Flapping setting:

Link Trap Threshold

The Link Trap threshold sets the number of SNMP link down traps that must be received within the Link Trap Window in order for InCharge to consider the port flapping. The default is 3. A value of 0 turns off flapping analysis.

Link Trap Window

The Link Trap Window sets the window of time used to monitor flapping analysis of a port. If the number of link down traps meets or exceeds the Link Trap Threshold during this window of time, the port is considered to be flapping. The default is 5 minutes.

A

Symptomatic Events

This appendix contains descriptions of symptomatic notifications. A symptomatic notification indicates an abnormal condition and is used by InCharge ATM/Frame Relay AM to diagnose root-cause problems. By default, the notifications are not subscribed to and do not display in your alarm log.

Containers

A container can be a card.

- *Operationally Down* indicates that a card's operational status is not in the *normal* state.

Systems

A system can be a switch.

- *Unresponsive* – Indicates that a system is not responding to status polls sent by the management station.
- *Might be Unavailable/Might be Unavailable No Loss* – Indicates that a system is unresponsive and is logically near the root-cause problem.
- *Excessive Restarts* – Indicates that too many system cold and warm start traps have been received within the restart trap window. Excessive Restarts is a symptom of a system unstable problem.

Service Access Points

A service access point can be an logical port.

- *Unresponsive* – Indicates that the endpoint on a service is unreachable.

Network Adapters

A network adapter can be a physical port.

- *Operationally Down* – Indicates that a physical port is down and is supposed to be up.
- *Flapping* – Indicates that too many link down traps have been received within the link trap window for a network adapter. Flapping is a symptom of a network adapter unstable problem.

Logical Links

A logical link can be a logical trunk.

- *Unresponsive* – Indicates that one or both logical ports connected to the logical trunk are down.

Connections

A connection can be a trunk cable.

- *Operationally Down* – Indicates that a trunk cable is not functioning properly. This notification is only available for devices that provide trunk cable instrumentation.

B

Diagnosis of Unstable Elements

This appendix describes how InCharge ATM/Frame Relay AM concludes that an element is unstable. A system or network adapter is considered to be unstable if it fluctuates too often between up and down states over a short period of time. InCharge monitors a system or network adapter's state via the SNMP traps it receives. InCharge determines when to send an Unstable Notification based on a combination of fixed values and user-controlled settings. InCharge also calculates a stable time in which to wait before clearing the Unstable Notification.

InCharge monitors the following SNMP traps to determine a change in an element's state:

- *Warm Start Traps* and *Cold Start Traps* for a system (that is, a switch).
- *Link Down Traps* for a network adapter (a port)

InCharge uses the following values to diagnose an element as unstable:

- *Minimum Traps* —This indicates the minimum number of Link/Restart Traps received in order to conclude that the element is unstable. This variable is set by the *Link Trap Threshold* parameter (contained in the Port Flapping setting) for network adapters and the *Restart Trap Threshold* parameter (contained in the Connectivity setting) for systems.

- *Trap Window* — This is the period within which the Minimum Traps must be received to declare the element unstable. This window is set by the *Link Trap Window* parameter (contained in the Port Flapping setting) for network adapters and the *Restart Trap Window* parameter (contained in the Connectivity setting) for systems. Once an element is declared unstable, InCharge computes the Stable Time.
- *Stable Time* — This is the amount of time that must elapse without further traps before InCharge declares the element stable again. Stable Time depends on the length of time the element was unstable. It is at least as large as that time, and at least as large as the Trap Window. However, it can be no longer than one hour.

Figure 11 illustrates how a system or network adapter is diagnosed as being unstable.

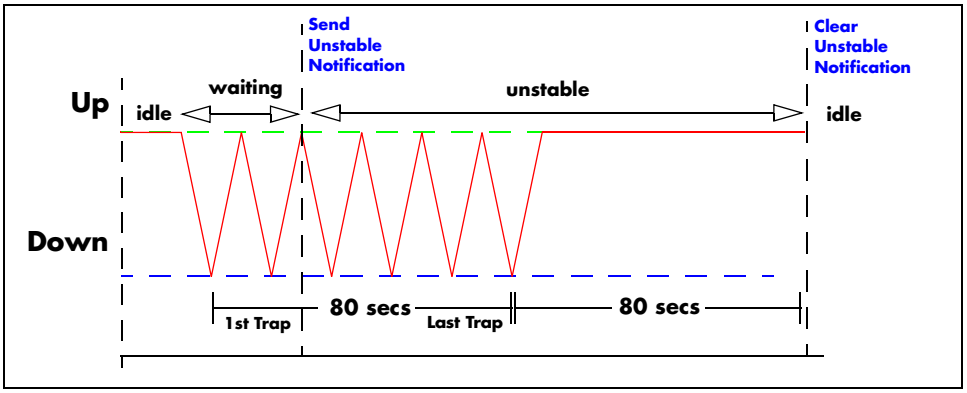

Figure 11: Unstable System/Network Adapter Diagnosis

In the example, let's assume the Link/Restart Trap Window parameter has a value of 30 seconds and the Link/Restart Trap Threshold parameter has a value of 2. InCharge would perform the following actions for the example:

1. As soon as InCharge receives a Link Down Trap from a physical port or (or a Warm Start/Cold Start Trap from a system), it begins counting.
2. When InCharge receives two or more traps within 30 seconds, the *Trap Window*, it considers the network adapter or system to be unstable and it sends an Unstable Notification. The *Minimum Traps* variable (set by the *Link/Restart Trap Threshold* parameter) determines the number of traps InCharge must receive (2) within the Trap Window (set by the *Link/Restart Trap Window* parameter) before it considers an element unstable.

3 InCharge continues to receive traps for 80 seconds after the initial trap. This results in a *Stable Time* of 80 seconds.

The Stable Time is the amount of time InCharge waits before it clears the Unstable Notification. In our example, the Stable Time is set at 80 seconds since it is greater than the *Trap Window* (30 seconds) and less than one hour.

As you can see, InCharge uses a relative measure to determine how long an element must be stable before it clears the Unstable Notification. This measure is proportional to the amount of time an element is unstable. The longer an element is unstable the longer it must be stable before the Unstable Notification is cleared. Because the element in our example remains stable for 80 seconds, InCharge clears the Unstable Notification no sooner than 80 seconds after it receives the final trap.

C

Alarms Processed

This appendix lists the alarms that can be processed by InCharge ATM/Frame Relay AM. The particular set of alarms processed by a given deployment depends on the network management infrastructure. For instance, InCharge ATM/Frame Relay AM does not process SNMP traps when the native Event Management System (EMS) is the sole source of the notifications.

Passport Alarms

The following table lists the Passport alarms that are processed by InCharge ATM/Frame Relay AM. (The information about the alarms is derived from Publication 241-5701-500: *Passport 6400, 7400, 15000 Alarms*.)

Alarm Group	Alarm Code	Alarm Meaning	Additional Description
0000	0000	This alarm clears all set alarms for components below. Also all related components for LP alarms	Hierarchical clear
0000	1000	For lockable components, it is locked or shutting down	DOS, LOS, or operational failure
0000	9000	An internal software error has been detected by the component	Software failure

Table 4: Passport Alarms Processed

Alarm Group	Alarm Code	Alarm Meaning	Additional Description
0999	0001	When status is "set", the Preside MDM workstation has lost the VC connection to the switch in question. It could be either a communication problem or switch failure	Unknown
0999	0012	The polled component has failed without a corresponding alarm from the network	Unknown
7000	0006	The CP is crashing because of an internal software problem	Software failure
7005	0204	Connection to DPN nodes is attempting to restage	DPNGATE failure
7005	0301	Trk failure due to congestion or faults	Lport failure
7006	0003	NMIS Telnet/FMIP/FTP Session failed because either killed, remote switch crashed, or IPIVC connection failed	Session failure
7006	0006	NMIS FMIP session has had 9 successive failed login attempts	Security violation
7007	0000	A DLCI on a FrAtm Lport has failed	VC failure
7007	1000	LMI failure messages exceeded threshold. May not be indicative of real connectivity failure	Lport failure
7007	2000	FrUni LMI failure (from the adjacent network)	Lport failure
7007	2010	FrUni LMI clear (from the adjacent network)	Lport clear
7007	2020	FrUni LMI failure (in the local network)	Lport failure
7007	2030	FrUni LMI clear (from the local network)	Lport clear
7011	2001	Indicates that the port is disabled due to the link condition	Pport link failure

Table 4: Passport Alarms Processed

Alarm Group	Alarm Code	Alarm Meaning	Additional Description
7011	5000	LOF state for greater than 2 seconds on the port. Applicable to EDS1, EE1, DS1 and E1 interfaces only	Pport link failure
7011	5001	RAI state indicating a LOF on the remote end. Applicable to EDS1, EE1, DS1 and E1 interfaces	Pport link failure
7011	5002	AIS state on the local port. Applicable to EDS1, EE1, DS1 and E1 interfaces	Pport link failure
7011	5003	LOS state for greater than 2 seconds on the port. Applicable to EDS1, EE1, DS1 and E1 interfaces only	Pport link failure
7011	5004	Multiframe RAI state indicating a frame alignment problem on the remote end. Applicable to EDS1, EE1, DS1 and E1 interfaces	Pport link failure
7011	5005	Red state for greater than 2 seconds on the local port. Applicable to EDS1, EE1, DS1 and E1 interfaces	Pport link failure
7011	5006	Yellow state for greater than 2 seconds on the local port. Applicable to EDS1, EE1, DS1 and E1 interfaces	Pport link failure
7011	5010	10 consecutive SES on the local port. Applicable to EDS1, EE1, DS1, and E1 interfaces	Pport link failure
7011	5011	Timing failing on the connection. Likely to cause framing errors	Pport link failure
7011	5100	LOS state for greater than 2 seconds on the port. Applicable to DS3 and E3 interfaces only	Pport link failure

Table 4: Passport Alarms Processed

Alarm Group	Alarm Code	Alarm Meaning	Additional Description
7011	5101	LOF state for greater than 2 seconds on the port. Applicable to DS3 and E3 interfaces only	Pport link failure
7011	5102	AIS state on the local port. Applicable to DS3 and E3 interfaces	Pport link failure
7011	5103	Far-end alarm received over FEAC channel. Only for C-parity mode	Pport link failure
7011	5104	DS3 Idle signal for more than 2 seconds	Pport link failure
7011	5110	Loopback request (far end)	Pport looped
7011	5111	Loopback request to loop local end	Pport looped
7011	5112	Loopback request to loop tributary	Pport looped
7011	5120	10 consecutive SES on the local port. Applicable to DS3 and E3 interfaces	Pport link failure
7011	5121	CBIT Unavailable due to 10 consecutive CSES on the local port. Applicable to DS3 and E3 interfaces	Pport link failure
7011	5122	Far-end unavailable state. Applicable to DS3 and E3 interfaces	Pport link failure
7011	5200	LOS state for greater than 2 seconds on the port. Applicable to SONET and SDH interfaces only	Pport link failure
7011	5201	LOF state for greater than 2 seconds on the port. Applicable to SONET and SDH interfaces only	Pport link failure
7011	5202	L-AIS state on the local port. Applicable to SONET and SDH interfaces	Pport link failure
7011	5203	L-RDI (Remote Defect Indicator) state. Applicable to SONET and SDH interfaces	Pport link failure

Table 4: Passport Alarms Processed

Alarm Group	Alarm Code	Alarm Meaning	Additional Description
7011	5210	Line Unavailable due to 10 consecutive L-SES. Applicable to SONET and SDH interfaces	Pport link failure
7011	5211	FEL-SES (Far-End Line Severely Errored Seconds) state. Applicable to SONET and SDH interfaces	Pport link failure
7011	5250	LOP state for more than 2 seconds on the local port. Applicable to SONET and SDH interfaces	Pport link failure
7011	5251	P-AIS (Path Alarm Indication Signal) state on the local port. Applicable to SONET and SDH interfaces	Pport link failure
7011	5252	P-RDI (Path Remote Defect Indicator) state. Applicable to SONET and SDH interfaces	Pport link failure
7011	5260	Path Unavailable due to 10 consecutive P-SES. Applicable to SONET and SDH interfaces	Pport link failure
7011	5261	FEP-SES (Far-End Path Severely Errored Seconds) state. Applicable to SONET and SDH interfaces	Pport link failure
7011	5501	Loss of Cell Delination on ATM interfaces. Many physical interface types possible	Pport link failure
7011	5701	G82 Far-End Unavailable state on the local interface. Applicable to E3 interfaces only	Pport link failure
7011	5702	G82 Unexpected payload type. Usually a misconfiguration	Pport link failure
7012	0052	One or more cards have failed	Card failure

Table 4: Passport Alarms Processed

Alarm Group	Alarm Code	Alarm Meaning	Additional Description
7012	0100	Card is unable to part of a logical processor because it has either failed or is being restarted	Card failure
7012	0101	Card reboot message issued after recovery. Indicates why the card went down	Card failure
7012	0102	The Card in question is now the active CP. Issued in failure of current active or Switch startup	CP Card switch
7012	0103	The power supply of the card has failed	Card failure
7012	0104	The power supply of the card has failed	Card failure
7012	0154	The card failed a self-test	Card failure
7012	0155	The card is unresponsive	Card failure
7012	0156	The card failed to insert into the backplane	Card failure
7012	0200	The Logical Processor has failed indicating that the active and spare cards have also failed	Card failure
7012	0202	The Logical Processor has switched from the active to the spare card	LP Card switch
7026	3000	Ethernet port failure	Pport failure
7039	1000	ATM Lport has detected that there are 1 or more troubled connections on this port	VC failure
7041	0050	The ILMI channel is down on this UNI port	UNI failure
7041	0150	The signalling channel is down for this UNI, IISP or PNNI port	Logical connection
7041	0250	Lport PNNI RCC down indicative of a loss of signal to the remote end	Logical connection

Table 4: Passport Alarms Processed

ALARM GROUP	ALARM CODE	ALARM MEANING	ADDITIONAL DESCRIPTION
7041	0251	The VCC used for the RCC channel has failed	Logical connection
7041	0252	The Hello protocol between the PNNI peers has broken	Logical connection
7041	0400	One or more SPVC or SPVP have been affected on this port	VC failure

Table 4: Passport Alarms Processed

Index

W